Université
De Boumerdes

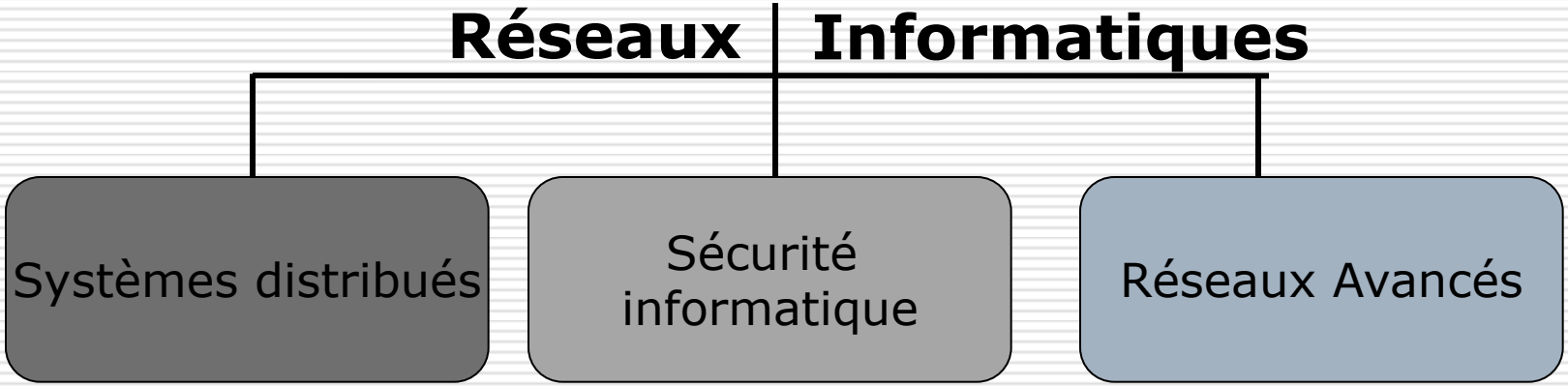
Université
De Limoges

Département d'informatique
M2

Introduction à la sécurité Informatique

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

Résultat Réseaux Informatique



- Rappels TCP/IP
- Client serveur (FTP, Telnet, SSH,…)
- Socket
- NFS
- RPC, CORBA, RMI
- Algorithmes distribués

- Routage avancé
- Réseaux Dynamiques:
- Réseaux Ad Hoc
- Réseaux P2P

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S5

Programme

Réalisé par : Dr RIAHLA

2008/2009

4 parties

- Introduction à la sécurité informatique
- Menaces (failles de sécurité, Attaques et vulnérabilités)
- Protections
- Gestion de la sécurité

Introduction
à la sécurité informatique

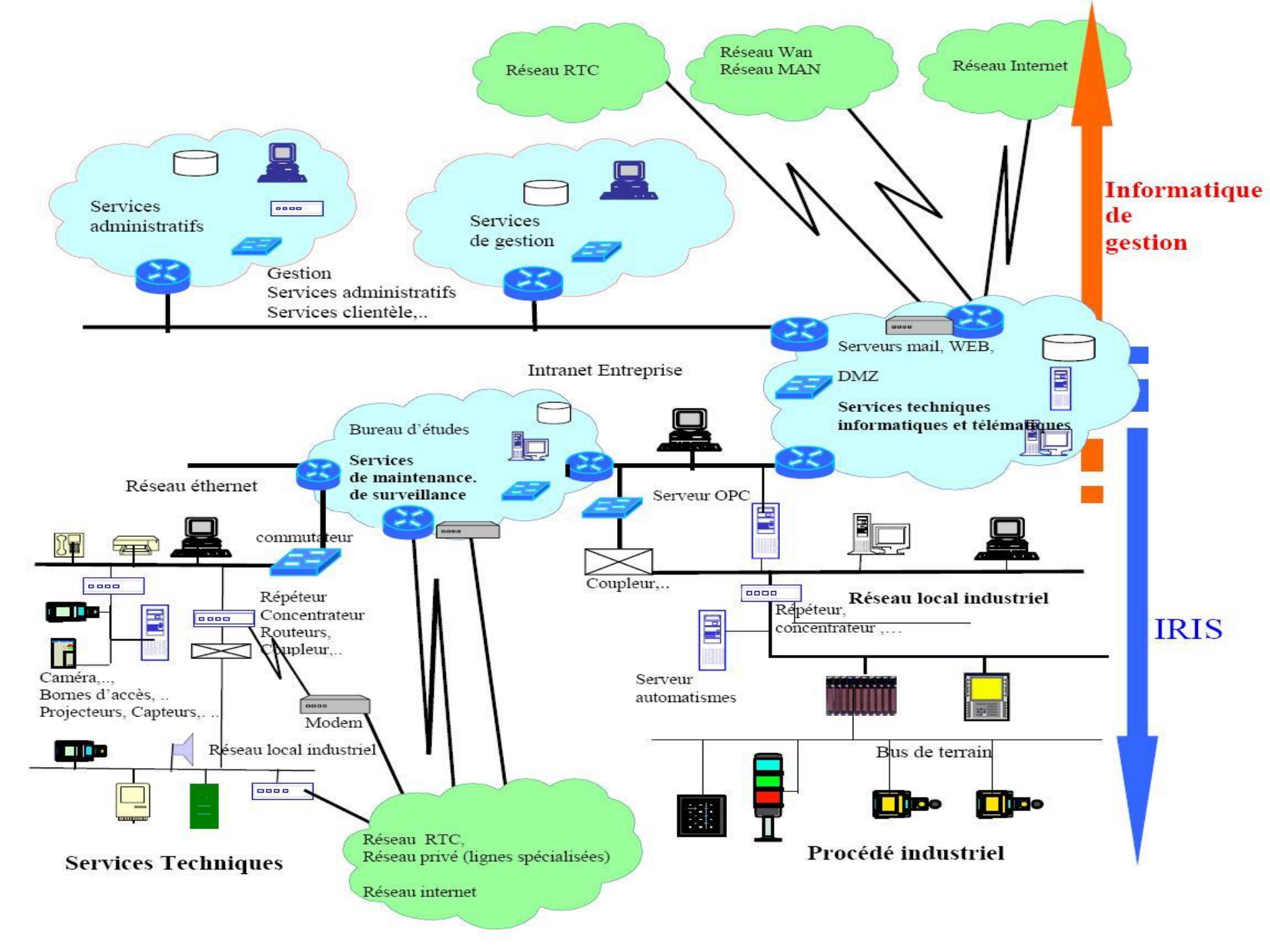
- **Introduction** (généralités et historiques).
- **Exigences fondamentales** et **objectifs** de la sécurité.
- Etude des **risques**.
- L'établissement d'une **politique de sécurité**.
- **Eléments** d'une politique de sécurité.
- Principaux **défauts** de sécurité.
- Notion **d'audit**.

Menaces
(failles de sécurité, Attaques et vulnérabilités)

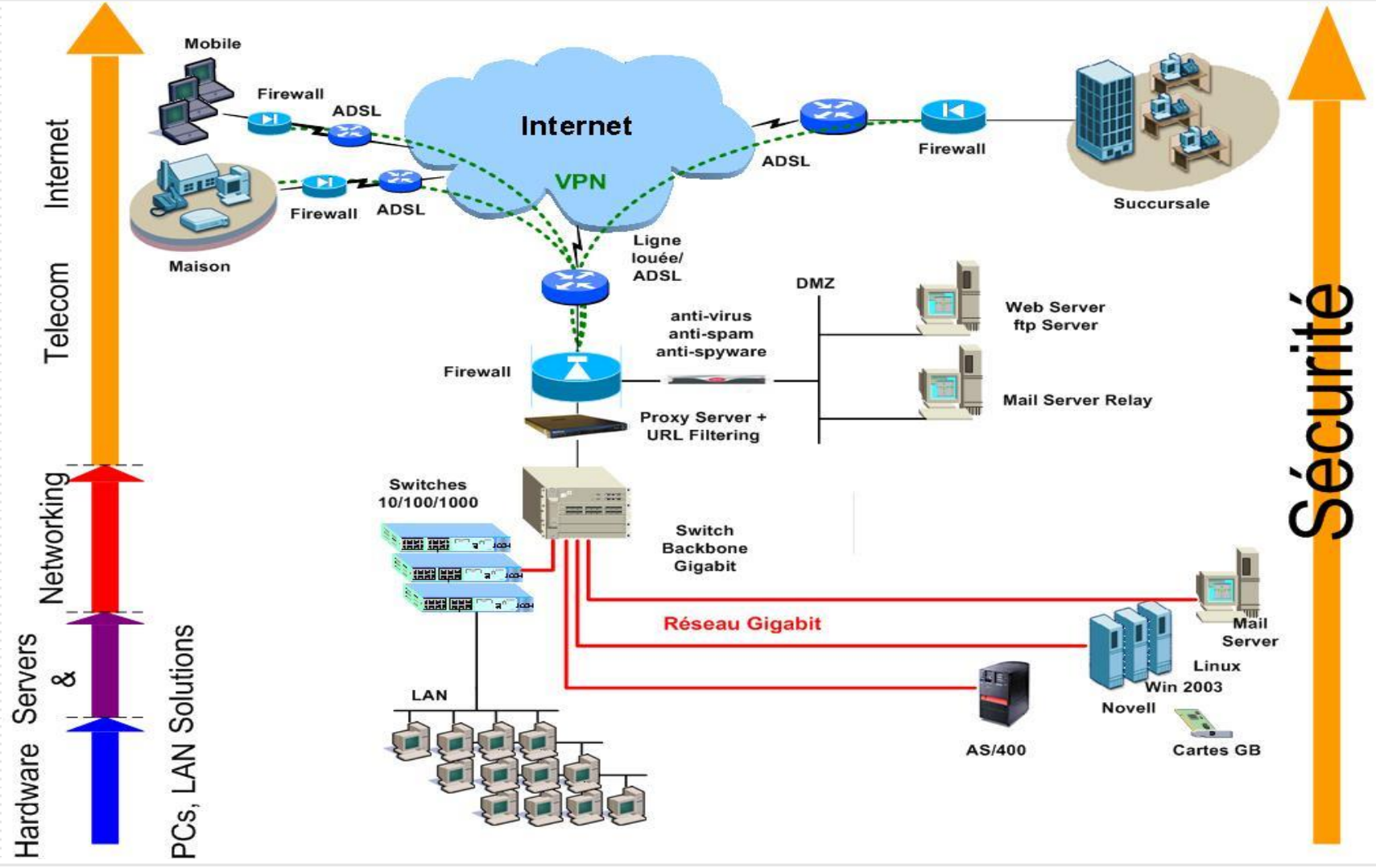
- Introduction
- Les différents types de vulnérabilités
- Virus, vers, chevaux de Troie et autres
- Vulnérabilités applicatives
- Vulnérabilités des réseaux
- Espionnage

Protections

- Formation des utilisateurs
- Poste de travail
- Antivirus
- Authentification et cryptage
- Pare-feu (firewall) : translation, filtrage et proxies
- Détection d'intrusion
- Communications et applications sécurisées
- VPNs

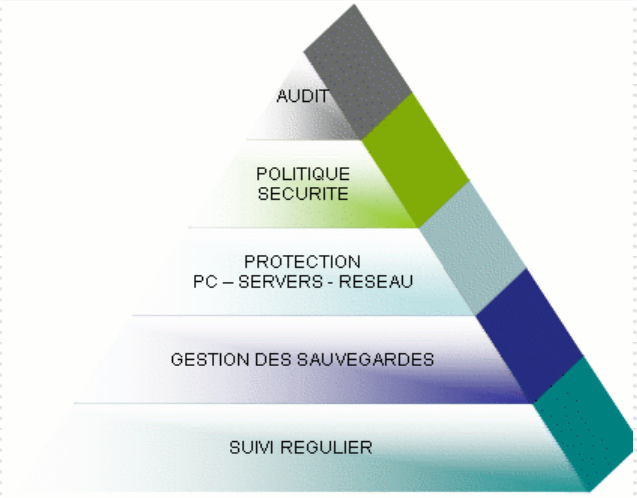

Réseau RTC
Réseau Wan
Réseau MAN
Réseau Internet
Informatique de gestion
Services administratifs
Services de gestion
Gestion
Services administratifs
Services clientèle,..
Intranet Entreprise
Serveurs mail, WEB,
DMZ
Services techniques informatiques et télématiques
Bureau d'études
Services de maintenance. de surveillance
Réseau éthernet
commutateur
Serveur OPC
Coupleur,..
Réseau local industriel
Répéteur, concentrateur ,…
Répéteur
Concentrateur
Routeurs,
Coupleur,..
Caméra,..,
Bornes d'accès, ..
Projecteurs, Capteurs,. ..
Modem
Serveur automatismes
Réseau local industriel
Bus de terrain
IRIS
Réseau RTC,
Réseau privé (lignes spécialisées)
Réseau internet
Services Techniques
Procédé industriel

Protections



Gestion de la sécurité

- Définition d'une politique de sécurité.
- Normes et standards de sécurité
- L'audit.



Objectif Principal

- **Connaissances générales** pour les non spécialistes
- **Une base** pour les futurs spécialistes de la Sécurité.

sécurité Informtique

Département de physique/Infotronique
IT/S5

Introduction à la sécurité informatique

Réalisé par : Dr RIAHLA

2008/2009

Réseaux Informtiques

Département de physique/Infotronique
IT/S5

1. Introduction (historique)

Réalisé par : Dr RIAHLA

Historique (**Kevin mitnick**)

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460921).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM -132
(Rev. 3/2/92)

November 1992

Historique (**Kevin mitnick**)

- Commencé à hacker des réseaux téléphoniques
- Il a attaqués les machines de **tsutomu shimomura** au centre du **supercomputing**

.

- Il a pénétré dans les serveurs du **WELL** et a accédé au courrier de **markoff** (un journaliste)

- Il a été arrêté avec l'aide d'annonce du **shimomura** et la société **WELL**

- A servi 5 années en prison et interdit d'utiliser des ordinateurs pour 2 années

Historique (**Kevin mitnick**)

- Il est maintenant Consultant en sécurité informatique.
- il a publié un livre traitant de **l'ingénierie sociale, IDS,…**

Historique (**DDOS**)

Février 2000

- Plusieurs sites Web majeurs non accessibles (ebay, cnn, amazon, microsoft,....) pour quelques heures.
- Ils sont inondés par un flux énorme de traffic (jusqu'à 1 gbps), de plusieurs adresses.

Février 16h

Quelqu'un est suspecté pour avoir lancé les attaques

Avril15h

il est arrêté au canada, il a 15 ans

Historique (**DDOS**)

Il a été condamné à 8 mois dans un centre de détention

Avec un programme automatique, il était capable de hacker 75 machines différentes dû à une vulnérabilité dans leurs serveurs ftp

il a installé un programme d'attaque distribué sur ces machines

Historique (**Autres**)

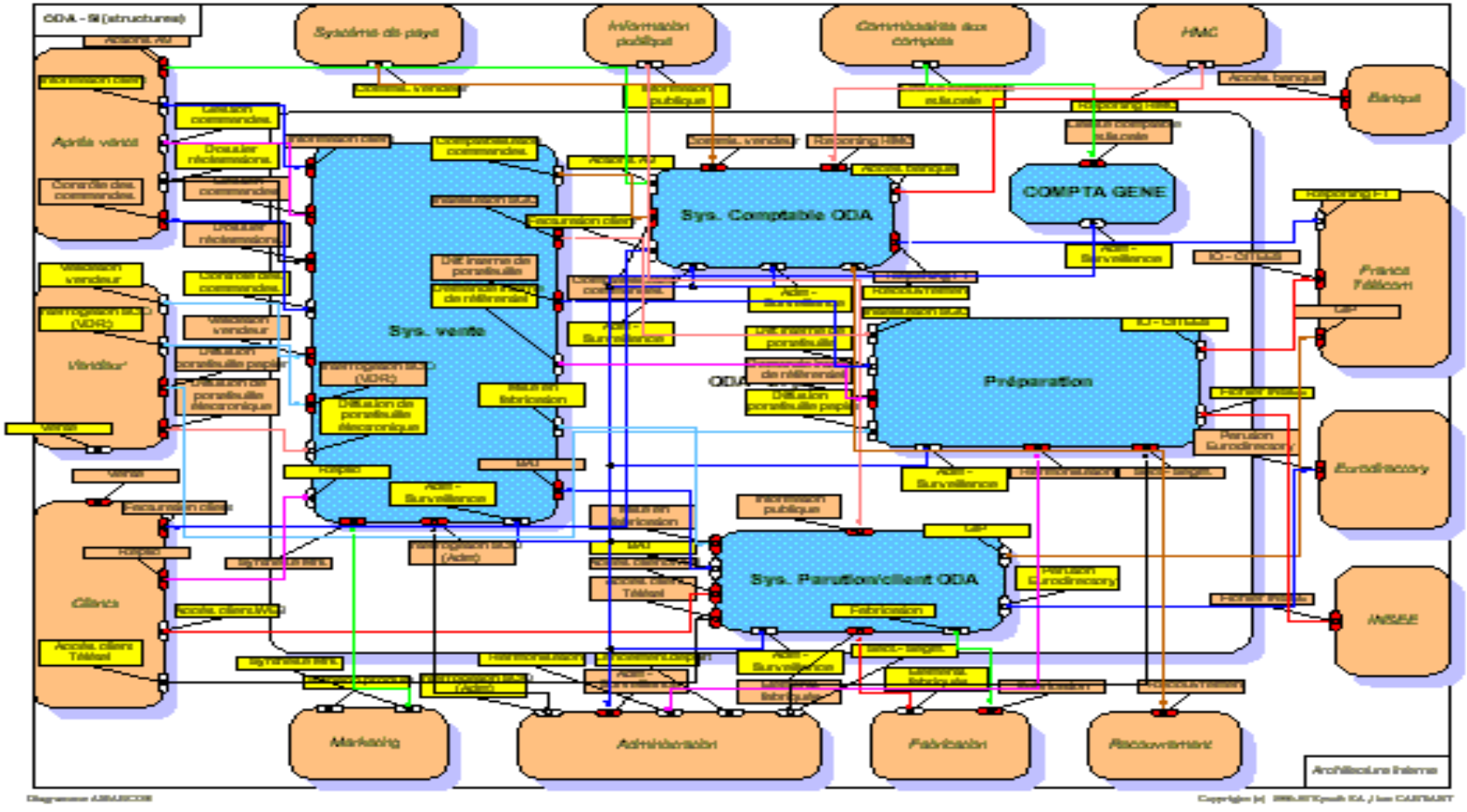
- MELLISA et autres bugs
- Programme de l'opération bancaire à distance.
- Virus, vers, spyware,…
- Attaques réseaux
- …etc

Systèmes d'information

- Un **système d'information** est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler.

- Organisation des activités consistant à **acquérir**, **stocker**, **transformer**, **diffuser**, **exploiter**, **gérer**... les informations.

Systèmes d'information



Systèmes d'information

– Besoin de plus en plus d'informations

• Grande diversitée dans la nature des informations:
– données financières
– données techniques
– données médicales
– …

• Ces données constituent les biens de l'entreprise et peuvent être très convoitées.

Systèmes Informatiques

- Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser **un système informatique (coeur)**.

- **Les Systèmes informatiques sont devenus la cible de ceux qui convoitent l'information.**

- **Assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques.**

Sécurité Informatique

- Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs **partenaires** ou leurs **fournisseurs**.

- Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Sécurité Informatique

- **La sécurité informatique** c'est l'ensemble des moyens mis en œuvre pour **réduire** la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

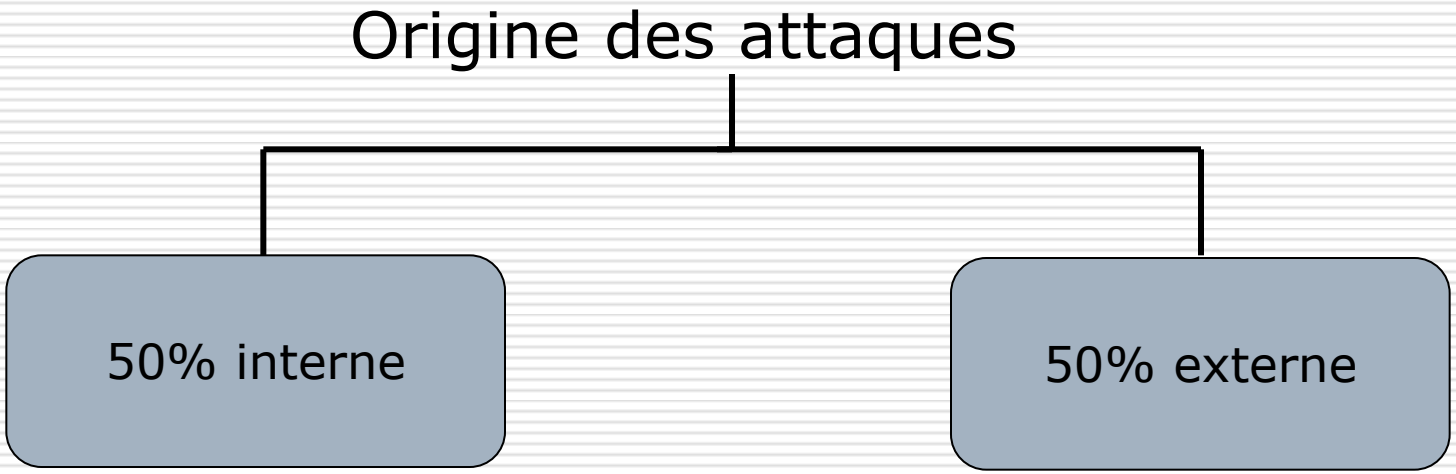
Réseaux Informtiques

Département de physique/Infotronique
IT/S5

2. Exigences fondamentales et objectifs

Réalisé par : Dr RIAHLA

Exigences fondamentales et objectifs



Exemple :
• utilisateur malveillant, erreur involontaire,…

Exemple:
• Piratage, virus, intrusion…,..

Exigences fondamentales et objectifs

- Elles caractérisent ce à quoi s'attendent les utilisateurs du systèmes informatiques en regard de la sécurité.

- La sécurité informatique vise généralement cinq principaux objectifs :

Exigences fondamentales et objectifs

- **L'intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être.

- **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

- **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information.

.

Exigences fondamentales et objectifs

La non répudiation, permettant de garantir qu'une transaction ne peut être niée.

L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

La sécurité recouvre ainsi plusieurs aspects :
respect de la vie privée (informatique et liberté).

Réseaux Informtiques

Département de physique/Infotronique
IT/S5

4. Étude (analyse) des risques

Réalisé par : Dr RIAHLA

Étude (analyse) des risques

- Il est nécessaire de réaliser une analyse de risque en prenant soin **d'identifier les problèmes potentiels avec les solutions** avec les **coûts associés.**

- L'ensemble des solutions retenues doit être organisé sous forme d'une **politique de sécurité cohérente**, fonction du niveau de tolérance au risque.

- On obtient ainsi la liste de ce qui doit être protégé.

Evolution des risques

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

Étude (analyse) des risques

- Quelle est la valeur des équipements, des logiciels et surtout des informations ?

- Quel est le coût et le délai de remplacement ?

- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs…).

- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Étude (analyse) des risques

Il faut cependant prendre conscience que les principaux risques restent :

- « câble arraché »,
- « coupure secteur »,
- « crash disque »,
- « mauvais profil utilisateur », …

Étude (analyse) des risques
Ce qu'il faut retenir

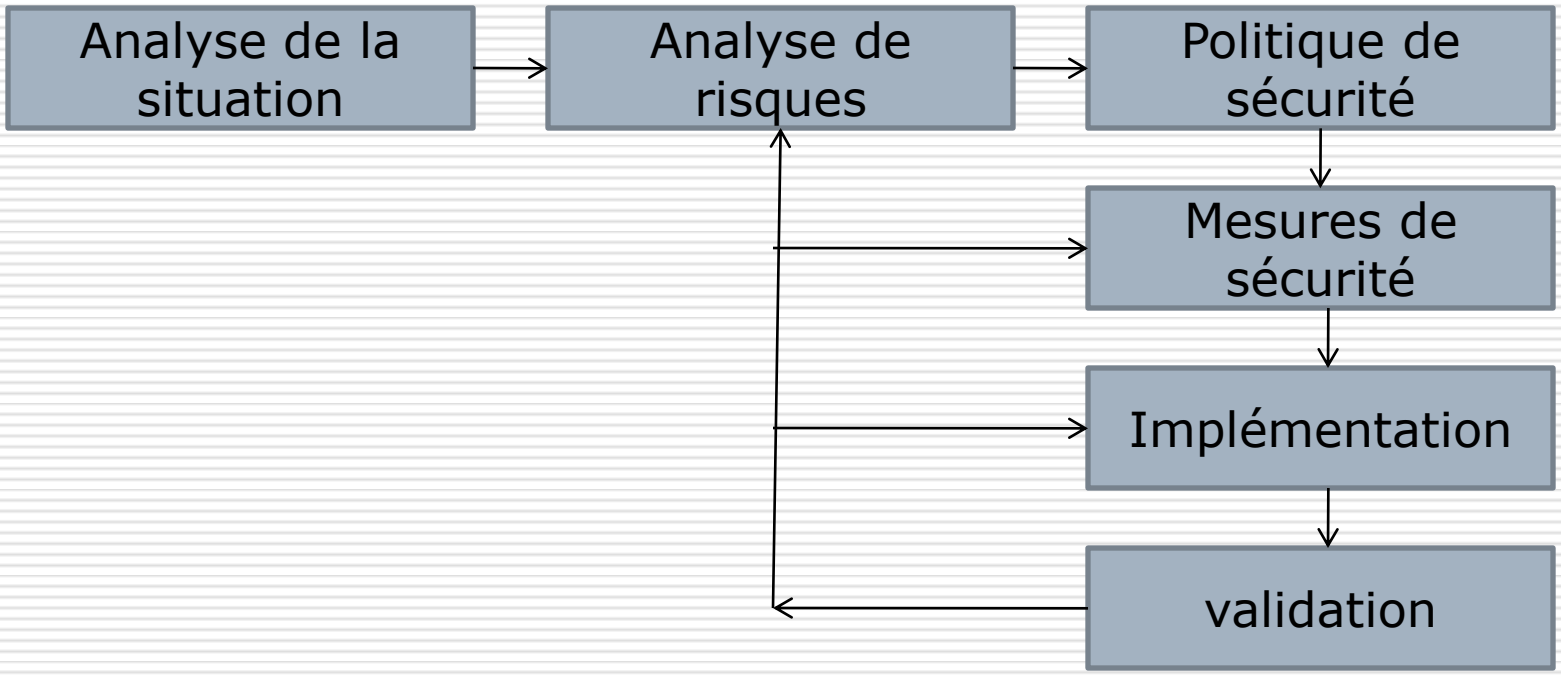
- Inventaire des éléments du système à protéger
- Inventaire des menaces possibles sur ces éléments
- Estimation de la probabilité que ces menaces se réalisent

Le risque « **zéro** » n'existe pas, il faut définir le risque résiduel que l'on est prêt à accepter.

4 parties

- Introduction à la sécurité informatique
- Menaces (failles de sécurité, Attaques et vulnérabilités)
- Protections
- Gestion de la sécurité

Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau



sécurité Informtique

Département de physique/Infotronique
IT/S5

5. Établissement d'une politique de sécurité

Réalisé par : Dr RIAHLA

2008/2009

Établissement d'une politique de sécurité

- Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible

- **Une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue**.

Établissement d'une politique de sécurité

Suite à **l'étude des risques** et avant de mettre en place des **mécanismes de protection**, il faut préparer une politique à l'égard de la sécurité.

Une politique de sécurité vise à définir les moyens de protection à mettre en œuvre

Établissement d'une politique de sécurité

- Identifier les risques et leurs conséquences.
- Elaborer des règles et des procédures à mettre en oeuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

Établissement d'une politique de sécurité

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez-vous avoir envers vous utilisateurs interne ?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?

Établissement d'une politique de sécurité

- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?

- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?

- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations ?

Établissement d'une politique de sécurité

Mise en œuvre

- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

sécurité Informtique

Département de physique/Infotronique
IT/S5

6. Éléments d'une politique de sécurité

Réalisé par : Dr RIAHLA

2008/2009

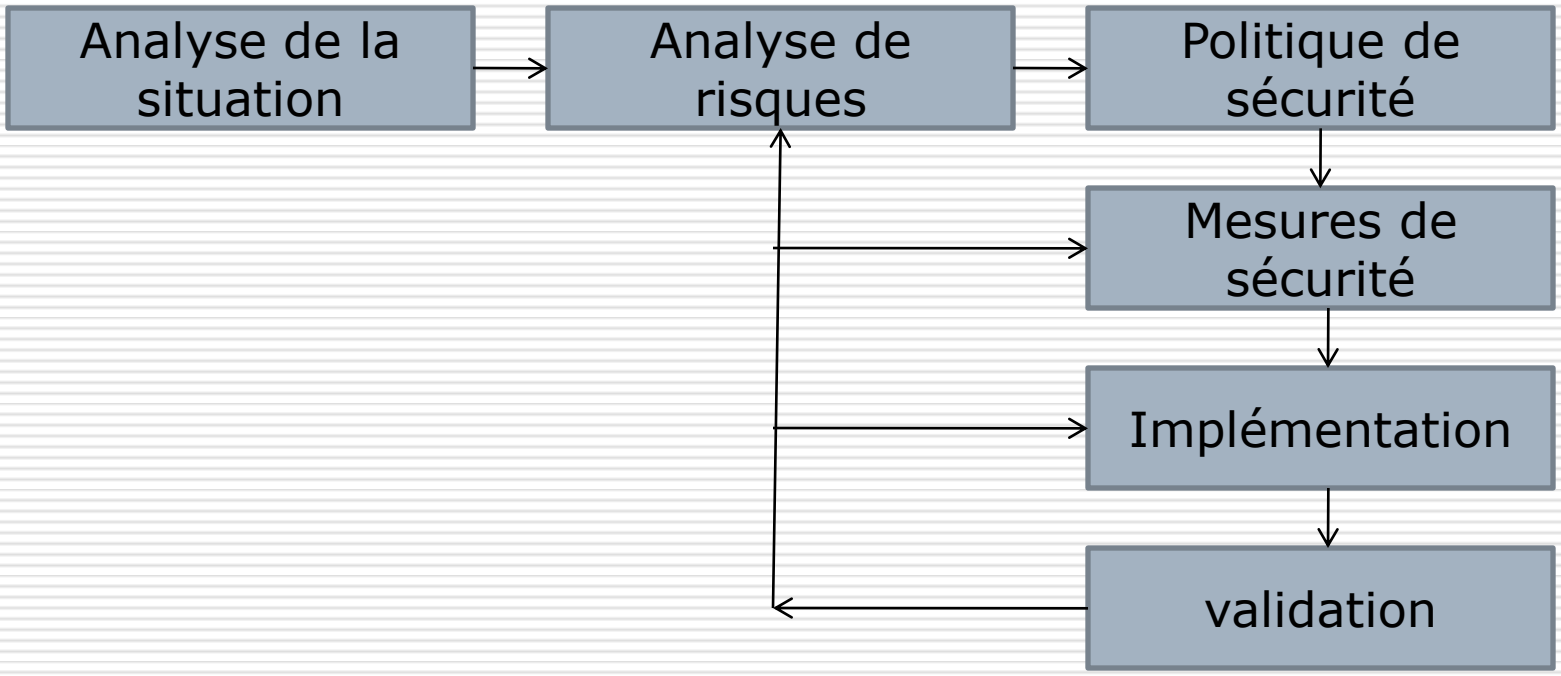
Éléments d'une politique de sécurité

- En plus de la formation et de la **sensibilisation permanente des utilisateurs**, la politique de sécurité peut être découpée en plusieurs parties :

Éléments d'une politique de sécurité

- **Défaillance matérielle** (vieillissement, défaut…)
- **Défaillance logicielle** (bugs, MAJ…)
- **Accidents** (pannes, incendies, inondations…)
- **Erreur humaine** (Formation)
- **Vol via des dispositifs physique** (disques et bandes), Contrôler l'accès aux équipements
- **Virus provenant de disquettes**
- **Piratage et virus réseau** (**plus complexe**)

Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau



Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau

Analyse de la situation : identifier le contexte du système à sécuriser.« *On ne sécurise pas de la même manière une maison, une banque ou une gare* »

Analyse des risques : (suite)
Diminuer le risque global auquel le système est exposé

Politique de sécurité :
Sert à décrire de quelle manière le risque global sera **diminué** (avec risque résiduel):

Décrire les différents éléments du système d'info et les règles qui s'y appliquent (classification des infos, découpage en zones, règles de protection pour chaque zone, etc…)

Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau

Mesures de sécurité :
Ensemble de mesures techniques (FireWall, Antivirus, IDS, …) ou **organisationnelles** (procédure de secours, nomination responsable sécurité, …) qui vont permettre d'appliquer la politique de sécurité

Implémentation
Installation et implémentation des différentes mesures

Validation
Validation des mesures implémentées afin de vérifier qu'elles offrent la protection voulue (Audits, scans de vulnérabilité, tests d'intrusion, etc…)

sécurité Informtique

Département de physique/Infotronique
IT/S5

7. Principaux défauts de sécurité

Principaux défauts de sécurité

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mises à jours non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (Netbios…).
- Traces inexploitées.

Principaux défauts de sécurité

- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Télémaintenance sans contrôle fort.
- Procédures de sécurité obsolètes (périmés).
- Authentification faible.

Principaux défauts de sécurité

l'état actif d'insécurité, c'est-à-dire la **non connaissance** par l'utilisateur **des fonctionnalités du système**, dont certaines pouvant lui être nuisibles (**par exemple** le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur)

l'état passif d'insécurité, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

Réseaux Informtiques

Département de physique/Infotronique
IT/S5

8. Notion d'audit

Notion d'audit

- Un audit de sécurité consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

- **L'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.**

Notion d'audit

Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres.

Merci